

# SecureTrust SAQ A Instruction Guide

**Purpose:** These instructions will assist in registering your account for PCI compliance, validating PCI Compliance readiness, and completing the annual PCI questionnaire when using Collect.js.

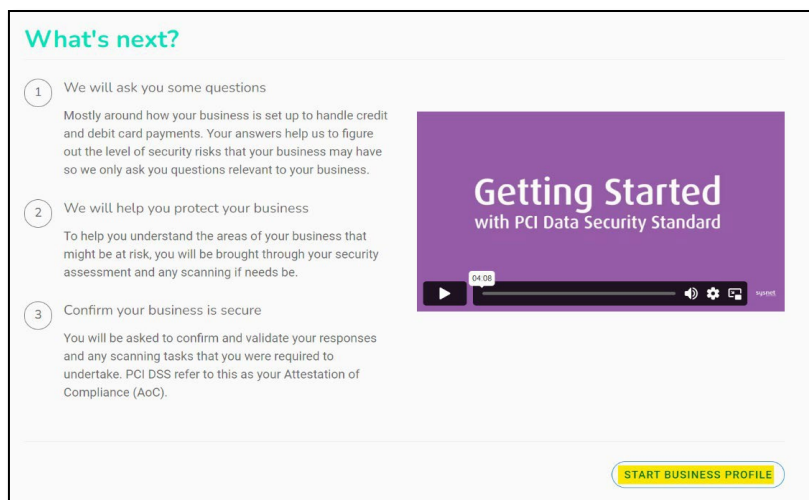
## Login & Registration

Use the log-in credentials in the preregistration email you received from SecureTrust.

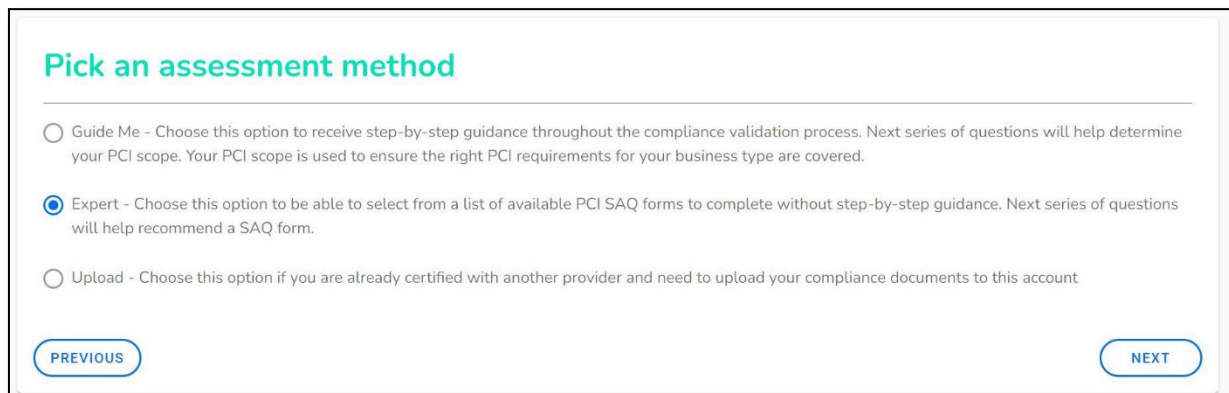
Click the **"Register Now!"** link, and use the information contained in the email to complete registration.

## Business Profile:

1. Once you have registered, you will begin completing the business profile. Click **Start Business Profile** in the lower right of this screen to begin.



2. On the following screen, choose **Expert** for the assessment method, and click **Next**.



3. This will display a listing of all the Self-Assessment Questionnaires (SAQ).

- Select **Self Assessment Questionnaire (SAQ) A**.
- Click **Next**.

### Your current valid PCI compliance type

Please select the PCI Compliance assessment type that you are currently valid for from the selection below.

- Self Assessment Questionnaire (SAQ) A
- Self Assessment Questionnaire (SAQ) P2PE
- Self Assessment Questionnaire (SAQ) B
- Self Assessment Questionnaire (SAQ) C-VT
- Self Assessment Questionnaire (SAQ) B-IP
- Self Assessment Questionnaire (SAQ) A-EP
- Self Assessment Questionnaire (SAQ) C
- Self Assessment Questionnaire (SAQ) D
- Self Assessment Questionnaire (SAQ) D-Service Provider
- Report on Compliance (RoC)

[PREVIOUS](#) [NEXT](#)

4. Answer the following Service Provider questions and click **Next**.

### Service Providers

Does your company share cardholder data with any third-party service providers (for example, Qualified Integrator & Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.)?

Yes  No

### Multiple Acquirer

Does your company have a relationship with more than one acquirer (e.g. merchant services provider, bank, etc.)?

Yes  No

[PREVIOUS](#) [NEXT](#)

- On the next screen, answer the free-form questions regarding how your business handles card payments.
  - Click **Next** when complete. All questions must be answered before moving to the next question.

### A summary of how and where you handle card payments

Please provide the information requested below. This will form part of your Attestation of Compliance

List your business premises type(s) and a summary of locations that are relevant to your PCI DSS assessment (eg, retail outlets, corporate offices, data centres, call centres etc.) ?

1/4000

Generally, how does your business store, process and/or transmit cardholder data? ?

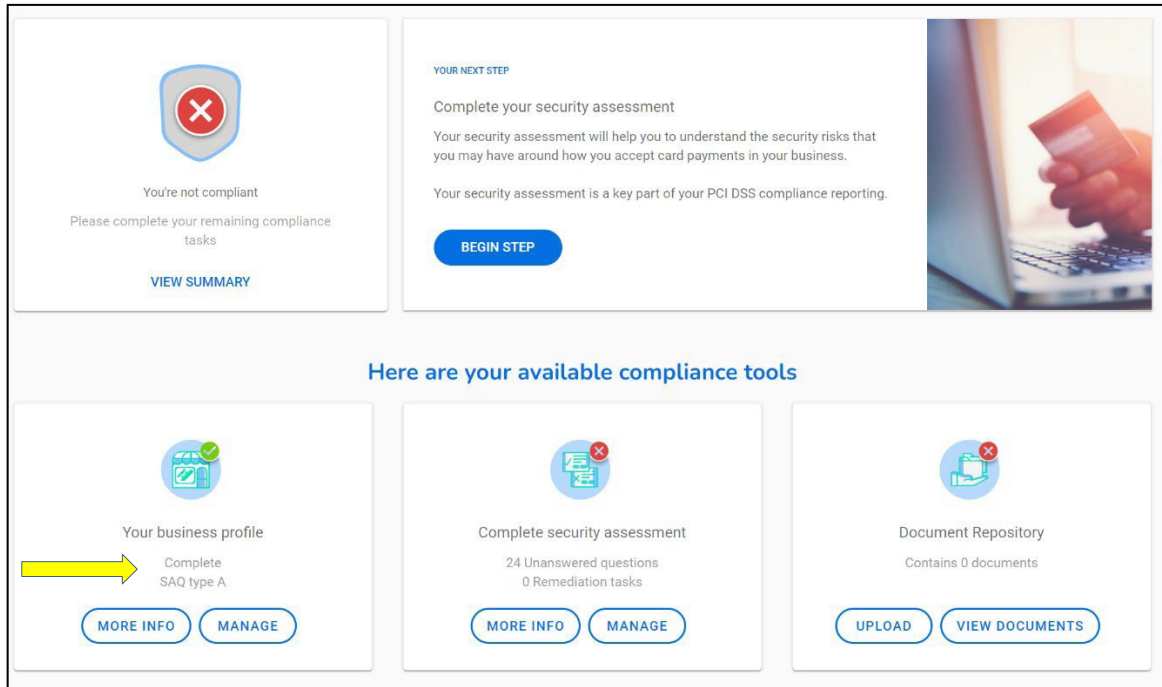
1/4000

Briefly describe the environment and/or systems covered by this assessment ?

1/4000

[PREVIOUS](#) [NEXT](#)

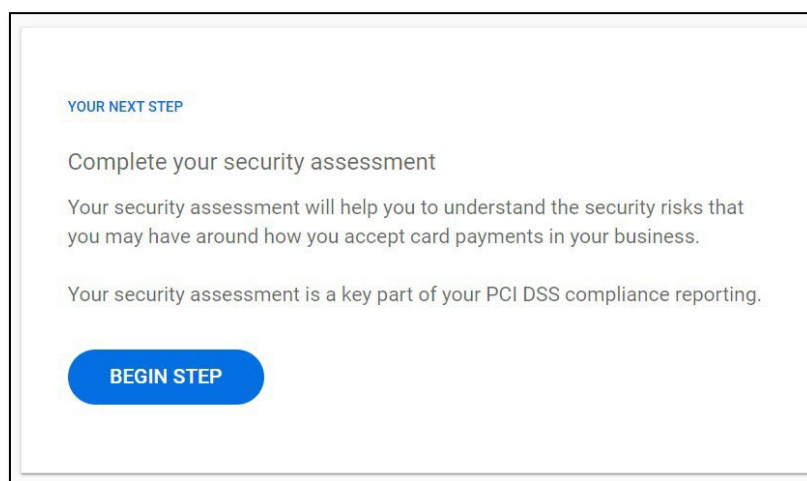
6. After clicking **Next**, the main PCI Dashboard will appear, and **Your Business Profile** should be marked as complete.
  - If this section does not display as complete, select **Manage** and review the section again for completeness.



The screenshot displays the PCI Dashboard interface. At the top left, a shield icon with a red 'X' indicates non-compliance. Below it, the text reads: "You're not compliant. Please complete your remaining compliance tasks." A "VIEW SUMMARY" link is provided. To the right, a "YOUR NEXT STEP" section titled "Complete your security assessment" explains that the assessment helps understand security risks and is a key part of PCI DSS compliance reporting. A "BEGIN STEP" button is located at the bottom of this section. Below these elements, a heading reads "Here are your available compliance tools". Three tool cards are shown: 1. "Your business profile" (Complete SAQ type A) with a yellow arrow pointing to it and "MORE INFO" and "MANAGE" buttons. 2. "Complete security assessment" (24 Unanswered questions, 0 Remediation tasks) with "MORE INFO" and "MANAGE" buttons. 3. "Document Repository" (Contains 0 documents) with "UPLOAD" and "VIEW DOCUMENTS" buttons.

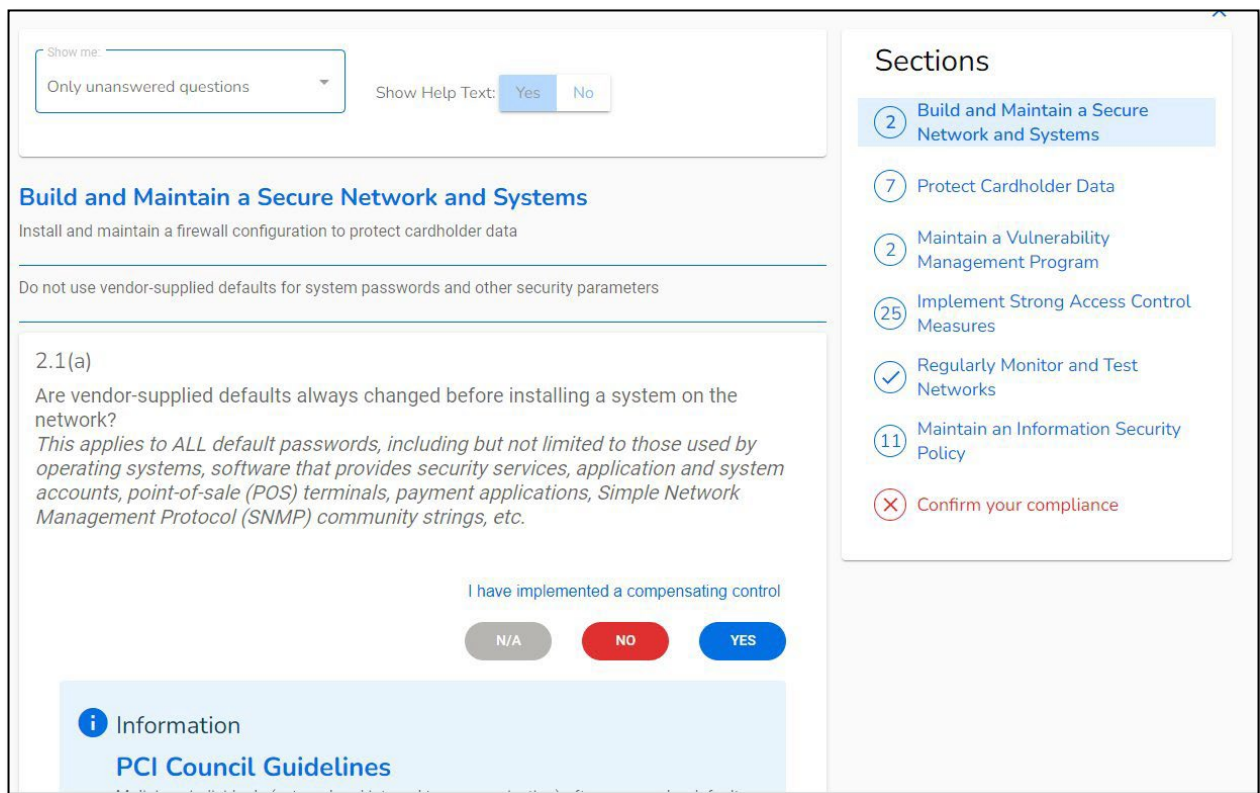
## Self-Assessment Questionnaire:

1. Complete the questionnaire by selecting **Begin Step**.



This screenshot shows a detailed view of the "YOUR NEXT STEP" section. It features the heading "Complete your security assessment" followed by two paragraphs of explanatory text: "Your security assessment will help you to understand the security risks that you may have around how you accept card payments in your business." and "Your security assessment is a key part of your PCI DSS compliance reporting." A prominent blue "BEGIN STEP" button is positioned at the bottom of the section.

2. The questionnaire will have **six** sections to complete.
  - As each section is complete, a teal check mark will replace the gray circles displayed in the “Sections” box below.
    - Note: The numbers in the box represent how many unanswered questions remain and will update as each question is answered.
  - Navigate through the questions by section. When a question is answered, it will automatically skip to the next required question to complete.



Show me: Only unanswered questions Show Help Text: Yes No

### Build and Maintain a Secure Network and Systems

Install and maintain a firewall configuration to protect cardholder data

Do not use vendor-supplied defaults for system passwords and other security parameters

2.1(a)  
Are vendor-supplied defaults always changed before installing a system on the network?  
*This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.*

I have implemented a compensating control

N/A NO YES

#### Information

PCI Council Guidelines

### Sections

- 2 Build and Maintain a Secure Network and Systems
- 7 Protect Cardholder Data
- 2 Maintain a Vulnerability Management Program
- 25 Implement Strong Access Control Measures
- ✓ Regularly Monitor and Test Networks
- 11 Maintain an Information Security Policy
- ✗ Confirm your compliance

3. After completing all six sections, confirm your compliance by reviewing the information in all the dropdown sections on this page:

### Confirm your compliance

Please review the form below and ensure all sections are correct and complete

- ✓ Your organization information details
- ✓ Type of business
- ✓ Description of environment
- ✓ Acknowledgement of status and attestation
- ✓ Merchant Executive Officer
- ✓ Attestation

[PREVIOUS](#)

4. Select **Confirm Your Attestation** to complete the SAQ.

✓ Attestation

✓ **Information for Submission.**

Based on the results noted in the SAQ P2PE dated Apr 1, 2022, the signatories identified in Parts 1.1, assert(s) the following compliance status for the entity identified in Part 2 of this document as of Apr 1, 2022:

Compliant: All sections of the PCI DSS SAQ are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby Wind River Test Account has demonstrated full compliance with the PCI DSS.

[CONFIRM YOUR ATTESTATION](#)

5. After confirming, it will redirect to the PCI Dashboard, where it will display a passing status compliance status.

The screenshot displays the PCI Dashboard interface. At the top left, a green shield icon with a checkmark is accompanied by a yellow arrow pointing to the text "You're compliant". Below this, it states "Valid until 22 December 2023" and provides two buttons: "VIEW SUMMARY" and "DOWNLOAD AOC". To the right, a message reads "YOU ARE NOW COMPLIANT" followed by "Congratulations, you're all done." and a coffee cup icon. Below this is a section titled "Here are your available compliance tools" containing three cards: "Your business profile" (Complete SAQ type A, with "MORE INFO" and "MANAGE" buttons), "Complete security assessment" (Last attested Dec 22, 2022, 8:59:34 AM, with "MORE INFO" and "MANAGE" buttons), and "Document Repository" (Contains 0 documents, with "UPLOAD" and "VIEW DOCUMENTS" buttons).